Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

GISRA Evaluation and Security Test and Evaluation

Mine Safety and Health Administration

FINAL REPORT

This review was performed by Pricewaterhouse Coopers LLP under contract to the Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

/s/

Assistant Inspector General for Audit

Report Number: 23-01-011-06-001
Date Issued: September 28, 2001

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Labor (DOL) and Mine Safety and Health Administration (MSHA) have developed and implemented many information security-related policies and procedures. However, MSHA needs to continue to strengthen its information security program. In particular, MSHA management needs to focus its attention and resources on implementing controls related to the following high priority areas: Risk Management; System Security Plan (SSP); Certification and Accreditation of Systems; Incident Response Capability; Identification and Authentication; Logical Access; and Audit Trails.

The FY 2001 Defense Authorization Act, Section X, Subtitle G, contains the Government Information Security Reform Act (GISRA), which requires the Inspector General (IG) or the independent evaluator, as determined by the IG, to evaluate DOL's mission-critical systems. In addition to the above requirement, the Office of the Inspector General (OIG) is required to conduct cyber security testing and evaluation (ST&E) in support of *Presidential Decision Directive* (PDD) 63 and in accordance with DOL's *Cyber Security Program Plan.* During the period of June through August 2001, PricewaterhouseCoopers (PwC) performed an evaluation of the implementation of the GISRA requirements by MSHA and an ST&E of MSHA's general support system (GSS) to determine how well the system security access controls enforce the agency's policy.

Implementation of security requirements were verified and validated against the National Institute of Standards and Technology's (NIST) *Self-Assessment Guide for Information Technology Systems* (Self-Assessment Guide), which encompasses requirements of GISRA, Office of Management and Budget (OMB) Circular A-130, General Accounting Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM), NIST Publications, and other Federal guidance.

An overview of the systems included in the GISRA evaluation and ST&E, our scope and methodology, and the summary results of our evaluations are described in the following sections of the report. The details of our findings are included in the "Findings and Recommendations" section of this report.

OVERVIEW OF SYSTEMS

The GISRA evaluation encompassed two MSHA major applications--Coal Management Information System (CMIS) and Mine Safety and Health Administration Part 50 System (Part 50 System).

CMIS is a mainframe-based application used to assist in monitoring and evaluating safety and health enforcement activities at the coal mines throughout the nation. This system collects and reports on information relating to the enforcement of safety and health regulations in coal mine operations. Data is processed relating to mine status, inspection, investigations, violations, citations, respiratory dust contaminants, and sampling. CMIS was custom developed in-house and is owned by the government. The application is written in Access while the database portion of the application is implemented using Common Business Oriented Language (COBOL 74 & 85), DML, IDS2, and DMIV TP.

The Part 50 System accomplishes the functions that are authorized by 30 USC 819. This system collects, edits, updates, stores, and reports information pertaining to mine operator and independent contractor identification, employment, accident, injuries, and fatalities chargeable to mine operators and contractors as defined in Part 50, 30 CFR. The system also provides statistical information.

The ST&E was performed on the MSHA LAN/WAN (MSHA's GSS). MSHA's GSS is a nationwide microcomputer network which encompasses five (5) major local area network (LAN) sites located at: (1) Arlington, VA; (2) Beckley, WV; (3) Lakewood, CO; (4) Pittsburgh, PA; and (5), Triadelphia, WV. These sites maintain connections to 14 district offices. The primary function supported by the MSHA's GSS is providing access to the agency's mine safety and health data, and enforcement statistics. This network provides direct connectivity for 19 MSHA sites around the nation.

It also provides processing for various administrative applications and data transfer adjuncts to mainframe applications. Much of this data is maintained on the agency mainframe computers and the Teradata information processed by the MSHA's GSS and is subject to the Privacy Act of 1974.

DESCRIPTION OF EVALUATIONS

Scope

The PwC team evaluated whether DOL and/or MSHA had promulgated policies and procedures that covered the GISRA requirements, as defined in the NIST Self-Assessment Guide. In addition, the team assessed the implementation of GISRA requirements for two MSHA major applications–CMIS and the Part 50 System. The evaluation of the implementation of GISRA requirements was assessed against the 212 questions listed under the following 17 control objectives in the NIST Self-Assessment Guide:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification & Accreditation)
- System Security Plan
- Personnel Security
- Physical and Environment Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

The PwC team also conducted an ST&E of MSHA's GSS through penetration testing to determine how well the system security access controls enforce the agency's policy. The objective of the ST&E was to assess the technical implementation of the security design and to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been implemented as required by the technical control objectives (i.e., Identification and Authentication, Logical Access Controls, and Audit Trails) in the NIST Self-Assessment Guide.

Methodology

Security requirements were reviewed and tested based on the NIST Self-Assessment Guide, as agreed to by DOL management, the OIG, and the PwC team. The PwC used an audit program, based on the NIST Self-Assessment Guide, to complete the following three phases:

Phase I: Planning

- Conduct entrance meetings with OIG officials, the DOL Chief Information Officer (CIO), and selected MSHA management officials

- Develop request lists of information required to complete project
- Develop proforma data collection instruments for agency staff interviews and other data collection needs
- Develop detailed work program to identify specific steps to complete the GISRA review and evaluations

Phase II: Verification and Testing

- Review and analyze documentation
- Conduct interviews
- Perform internal and external penetration testing to:
  - Determine if security defenses sufficiently protected the network
  - Identify network topology/vulnerabilitie s
  - Use the topology and system vulnerabilities to determine if unauthorized access to internal network is possible
  - Demonstrate identified vulnerabilities
- Document GISRA evaluation and ST&E results
- Prepare work-papers and perform supervisory review

Phase III: Reporting

- Conduct meetings with appropriate staff regarding tentative findings
- Complete Tentative Findings Report--Combine GISRA evaluation and ST&E findings
- Perform supervisory review
- Respond to OIG review
- Hold meeting with agency management to discuss the results and recommendations for corrective action.
- Respond to agency review
- Revise Tentative Finding Report and issue Draft Report
- Hold closing meeting with OIG to deliver Final Report

EVALUATION SUMMARY

We found that overall the Department and MSHA have promulgated policies and some procedures covering all of the 17 control objectives in the NIST Self-Assessment Guide. However, additional procedures are needed for the following 12 control objectives:

- Review of Security Controls
- System Security Plan
- Personnel Security
- Physical Security and Environmental Controls
- Production, Input/Output Controls
- Hardware/System Software Maintenance
- Data Integrity
- Documentation
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

We also reviewed MSHA's implementation of the 17 control objectives in the NIST Self-Assessment Guide. While MSHA has implemented many of the requirements under the control objectives, there are still requirements that have not been implemented for each of the 17 control objectives.

While all areas are considered important, the table below identifies the control objectives we considered high and medium priority based. For purposes of assessing priorities for each control objective, we used the following criteria:

High Priority: Control objectives that are characterized by the following: (1) inherently high risk; (2) DOL or agency procedures are limited; or (3) implementation of the procedures is limited.

Medium Priority: Control objectives that are still important, but do not meet the above criteria.

Control Objective Category	High Priority	Medium Priority
Management Controls		
Risk Management		X
Review of Security Controls		X
Life Cycle		X
Authorize Processing (Certification and Accreditation)	X	
System Security Plan		X
Operational Controls		
Personnel Security		X
Physical and Environmental Protection		X
Production, Input/Output Controls		X
Contingency Planning	X	
Hardware and System Software Maintenance		X
Data Integrity		X
Documentation	X	
Security Awareness, Training and Education		X
Incident Response Capability	X	
Technical Controls		
Identification and Authentication	X	
Logical Access Controls	X	
Audit Trails	X	
Total	7	10

MANAGEMENT COMMENTS

In response to the draft report, MSHA generally concurs with the findings and recommendations and identified some actions taken and planned to address the recommendations. However, MSHA stated that resources will not be allocated to implementing security controls over CMIS or the Part 50 System, since those systems are being replaced. In addition, MSHA responds that it does not intend to redirect any resources toward changes to input/output controls on either the Honeywell or the IBM mainframe, because those platforms will be shut down in November 2002 and January 2003, respectively.

MSHA is in the process of developing the MSHA Standardized Information System (MSIS). The MSIS is a web-based application with an Oracle database.

The MSIS integrates and modernizes all of MSHA’s legacy mainframe systems. CMIS and the Part 50 System development are frozen and no modifications will be made except those that are legislatively mandated. CMIS and the Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the Calendar Year 2002.

MSHA's comments to the draft report are summarized under the "Management Comments" section for each finding. MSHA's complete response to the draft report is included in its entirety as Appendix A to this report.

CONCLUSION

The actions planned by MSHA, when fully implemented, should satisfy the intent of some of the recommendations. However, MSHA does not provide target dates for the many of the planned actions.

MSHA responded that it did not intend to allocate additional funding and personnel to implement security controls over CMIS and the Part 50 System since they are being replaced as part of the MSIS project. In addition, MSHA responds that it does not intend to redirect any resources toward changes to input/output controls on either the Honeywell mainframe or the IBM mainframe, because those platforms will be shut down in November 2002 and January 2003, respectively, as part of the MSIS project. The MSIS project is a major system effort and complexities and deadline set backs are inevitable. Historically, major system development projects have seldom met projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, adequate security controls related to CMIS and the Part 50 System and adequate input/output controls related to the Honeywell and IBM mainframes will not be implemented for potentially several years. However, MSHA management is aware of the risks, and despite the risks, has decided not to devote any additional resources to these areas.

We provided comments and conclusions under the "Conclusion" section for each of the findings.

FINDINGS AND RECOMMENDATIONS

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.1.1)

Risk Management

Condition:
The CIO’s Computer Security Handbook (CSH) provides the risk management policies and procedures to be followed by the DOL agencies.

Risk assessments have been performed for CMIS (CMIS is part of the Mine Safety and Health Training and Enforcement System and was included in the risk assessment of that system) and the Part 50 System. However, MSHA has not fully implemented the risk management requirements. In particular, MSHA has not:

- Performed and documented risk assessments on a regular basis.
- Documented and maintained on file the management approvals on the final risk determinations.
- Conducted a mission/business impact analysis subsequent to the recent risk assessment process.
- Conducted a countermeasure analysis that determines whether the security requirements in place adequately mitigate vulnerabilities.

Cause:
Prior to the 2001 risk assessments, the risk assessment process was not a high priority with MSHA. While MSHA has taken significant actions to implement the risk management requirements, it has not prepared a detailed plan of action to identify and prioritize the specific steps of implementation of the selected safeguards which could reduce or eliminate the vulnerability of the systems to the threats.

Criteria:
The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act (GISRA)* section 3534 states that, “. . . Appropriate senior agency officials are responsible for assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control . . . .”

The Federal Manager's Financial Integrity Act of 1982 requires agencies to conduct risk assessments to identify and prioritize their vulnerabilities to waste, fraud, and abuse.

OMB Circular A-130 Appendix III, requires that agencies consider risk when determining the need for and selecting computer-related control techniques. Appendix III states “. . . The risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards . . . .”

FISCAM SP-1 states that successful risk assessment programs require final sign-off by business managers indicating agreement with risk reduction decisions and acceptance of residual risk and that these approvals should be documented and maintained on file.

NIST 800-30, *Risk Management Guide (1st Public Exposure Draft)*, states that, “. . . that new risks will periodically surface and risks previously mitigated will again become a concern. Thus, the risk management process is ongoing and evolving.

There should be a specific schedule, but the process should also be flexible enough to allow changes where warranted. As a rule of thumb, the analysis is usually repeated within 24 months or less…It is the process owner’s responsibility to make the final decision about the degree of risk they are willing to accept…a major step in the risk assessment process is to determine the mission impact resulting from the threats . . . ."

The CSH, chapter 3, p.10 states that "…during the operation phase of the IT system, a risk assessment (RA) should be conducted periodically on the system . . . to determine the extent to which existing security safeguards meet security requirements . . . Identify alternate security safeguards that will mitigate the effects of the risks generated by threat/vulnerability pairs . . . .”

The DOL Cyber Security Program Plan (CSPP), chapter 7, *section B, p.7* states, “. . . All DOL IT systems will have up-to-date Vulnerability Assessment (VAs) or Risk Assessments (RAs) . . . .”

Effect:
The absence of a current and clear understanding by program officials of the vulnerabilities of its systems limits the ability of MSHA to make timely decisions to mitigate risks to the MSHA mission and ability to carry on its normal business operations. Thus, effective security controls needed to ensure that the information in MSHA's systems is adequately protected and can be relied upon for decision-making may not be implemented

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meetrisk management requirements.

Management Comments:
MSHA plans to complete all components of the MSHA Computer Security Handbook in FY 2002. One of the components of the handbook is the Vulnerability Assessment Guide. The MSHA responsibilities included in the handbook are:

- Conducting risk assessments of MSHA’s cyber-based systems as required by the DOL CIPP/PPD-63 and OMB A-130.
- Developing further threats, questions or assess valuation guidance for MSHA’s sites and documenting them as necessary.
- Acquiring sign-off by business managers.
- Conducting a risk assessment on a 24-month schedule or a schedule set by the DOL OCIO or when significant modifications have been made to a system.

Conclusion:
The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not specifically address the implementation of the risk management requirements and target dates for implementation.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.1.2) **Review of Security Controls**	**Condition:** The CSH provides policy guidance to the DOL agencies regarding conducting periodic reviews of security controls. However, the following procedures are not specifically addressed in the DOL or MSHA guidance documents: • Review the operating system periodically to ensure the configuration prevents circumvention of the security software and application controls. • Routinely conduct tests and examinations of key controls (i.e., network scans, analyses of router and switch setting, penetration testing). • Analysis and take remedial actions on all security alerts and security incidents. • Implement a process for reporting significant weakness and ensuring effective remedial action. Recently, the Information Security Office (ISO) implemented network reviews. The ISO INFOSEC Engineer routinely evaluates the network for potential weakness, and reports them for correction. However, MSHA has not: • Prior to the recent implementation of INFOSEC Engineer reviews, MSHA had not performed periodic reviews on two of their major application systems: CMIS and Part 50 System. • Conducted an independent review or routine self-assessments on these systems in the past three years. SRA International conducted a penetration test last year, however, the systems residing on the Honeywell Mainframe (CMIS) and SunGard Mainframe (the Part 50 System) were out of bounds for the test. • Put into place a process for reporting significant weaknesses and ensuring effective remedial actions. • Implemented routine tests and exams of key controls (i.e., network scans, router and switch setting analysis, penetration testing). **Cause:** Prior toY2K, system security was not a high priority with MSHA. Management officials cited the lack of resources and personnel to conduct periodic security reviews. Currently, there is only one full-time employee in the information security area. However, MSHA has not completed adequate analyses to determine the resources necessary and has not developed action plans to issue procedures and fully implement requirements related to conducting security reviews. Also, prior to 2001 management of information security was decentralized in MSHA, which further inhibited consistent procedures and implementation of information security requirements. This problem has been resolved through the implementation of a centralized Information Security Office in January 2001. MSHA has made many improvements to their security posture since the FY 2000 FISCAM audit. However, MSHA has decided not to allocate additional funding and personnel to perform periodic reviews of security controls of the legacy systems (CMIS and the Part 50 System) since they will be replaced by the new MSHA Standardized Information System (MSIS). The MSIS project is a major system effort and complexities and deadline set backs are inevitable.

Although there is a MSIS Project Plan in place, MSHA cannot be assured that MSIS will be fully implemented by its proposed date. As such, MSHA should continue to practice information security and perform periodic reviews of security controls for its legacy systems.

Criteria:
The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act (GISRA)*, requires that the head of each agency ensure periodic testing and evaluating of information security controls and techniques and implement appropriate remedial actions based on the evaluation. In addition, GISRA requires that each agency shall have an annual independent evaluation of the information security program and practices of that agency.

OMB Circular A-130 requires that agencies perform an independent review or audit of the security controls in each application at least every three years or sooner, if significant modification have occurred or where the risk and magnitude of harm are high.

FISCAM SP-5.1 states that "… Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan . . . ."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* states that ". . . Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software "patches"), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every three years . . . ."

The CSH states that "…An independent review of security controls for each Major Application System should be performed at least every three years … the results of the review conducted should be analyzed. Include specifics on who conducted the review. If any recommendation or findings were made as a result of the review, the outcome should be addressed . . . ."

Effect:
Although the application systems will be migrated to the client-server environment starting September 2001, the MSIS project will not be completed until 2003. Therefore, in the interim, effective security controls may not be in place to prevent or detect unauthorized or inappropriate access to MSHA's sensitive systems and information during this period. Furthermore, major system development projects historically have incurred delays well beyond projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, MSHA's sensitive systems and data may be at risk for much longer than 2 years.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to complete future security reviews and evaluations and fully meet other review of security control requirements.

Management Comments:
MSHA’s Configuration Management process, and the security policy placed on MSHA’s “Core Load” mandate controls over the operating system. The same CM requirements are applied to the other components of the network.

The MSHA Information Security Office (ISO) reviews major security alerts and is involved in the implementation of these alerts. MSHA’s process for implementing alerts from all sources is under development. Additionally, the ISO INFOSEC Engineer routinely evaluates the network for potential weakness, and reports them for correction.

MSHA is in the process of developing the MSHA Standardized Information System (MSIS). The MSIS is a web-based application with an Oracle database. The MSIS integrates and modernizes all of MSHA’s legacy mainframe systems. CMIS and the Part 50 System development are frozen and no modifications will be made except those that are legislatively mandated. The first release of an SSP for the MSIS is scheduled for September of 2001. CMIS and the Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the calendar year 2002. The scheduled shutdown for the Honeywell is 11/02 and the IBM is 01/03. Therefore, resources won’t be allocated to perform periodic reviews of CMIS and the Part 50 System.

Conclusion:
MSHA does not address the development of procedures identified in this finding to bring MSHA into compliance with the NIST requirements.

In addition, MSHA responds that it does not intend to allocate additional funding and personnel to perform periodic reviews of security controls of CMIS and the Part 50 System since they will be replaced by MSIS. As we stated earlier, the MSIS project is a major system effort and complexities and deadline set backs are inevitable. Historically, major system development projects have seldom met projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, the security controls related to CMIS and the Part 50 System will not be subjected to any review process for potentially several years.

MSHA management is aware of the risks, and despite the risks, has decided not to devote any additional resources to security controls to CMIS and the Part 50 System. We are not contesting management's position.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.1.3) **Life Cycle**	**Condition:** The DOL *Systems Development and Life Cycle Management Manu*al (SDLCM) provides the life cycle policies and procedures to be followed by all DOL agencies. In addition, MSHA has promulgated additional change management guidance. We reviewed the implementation of life cycle requirements for the CMIS and the Part 50 System. However, these systems were developed in house by MSHA in the late 1970's and early 1980's. As such system documentation is unavailable and we are unable to assess MSHA's compliance with life cycle requirements in the initiation, development, and implementation phases. Thus, for implementation the scope of our review was limited to the operations/maintenance and disposal phases. During these phases MSHA did not periodically review the SSPs of CMIS and the Part 50 System and adjust the SSPs to reflect current conditions and risks. **Cause:** MSHA has decided not to allocate additional funding and personnel to perform additional security tasks for the legacy systems (CMIS and the Part 50 System) since they will be replaced by the new MSHA Standardized Information System (MSIS). The MSIS project is a major system effort and complexities and deadline set backs are inevitable. Although there is a MSIS Project Plan in place, MSHA can not be assured that MSIS will be fully implemented by its proposed date. As such, MSHA should continue to review and update its SSPs for CMIS and the Part 50 System. **Criteria:** The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA) states that the head of each agency shall ensure that the agency's security plan is practiced throughout the life cycle of each agency system. OMB Circular A-130 states that agencies shall establish information system management oversight mechanisms that ensure major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources. NIST 800-27, *Engineering Principles for Information Technology Security*--this recently released publication (June 2001) presents security principles and their relationship/applicability to each phase of life cycle development. NIST 800-30, *Risk Management Guide (Draft)*, states that all security-related activities are a part of the risk management process and that risk management spans the entire system development life cycle(SDLC). The CSH requires MSHA to update the SSP as the system progresses throughout its life cycle.

Effect:
CMIS and the Part 50 System contain sensitive information to include Privacy Act data, that requires adequate security controls to mitigate risk of unauthorized disclosure, disruption, modification or destruction of information collected or maintained by the agency. In the absence of an updated SSP for CMIS and the Part 50 System, MSHA cannot be assured that information security is practiced throughout the final stages of the systems' life.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to review and update the SSPs for CMIS and the Part 50 System.

Management Comments:
MSHA is in the process of developing the MSHA Standardized Information System (MSIS). The MSIS is a web-based application with an Oracle database. The MSIS integrates and modernizes all of MSHA's legacy mainframe systems. CMIS and the Part 50 System development are frozen and no modifications will be made except those that are legislatively mandated. The first release of an SSP for the MSIS is scheduled for September of 2001. CMIS and Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the Calendar Year 2002. The scheduled shutdown for the Honeywell is 11/02 and the IBM is 01/03.

The MSIS development team is following the requirements of all five life cycle phases contained in the DOL SDLC manual. The SDLC contains security requirements such as assessing project risks, developing the SSPs and conducting Security Risk Assessments. The SDLC also provides policy and procedures for maintaining the security requirements. In addition, the MSHA Security Work Plan covering FY 2001 and FY 2002 contains detailed plans and timeframes for writing security policy and procedures covering additional DOL security requirements. The initial SSP for the MSIS is scheduled for September 2001 completion. The Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the calendar year 2002.

MSHA developed and implemented *System Change Management Guidelines* in June 2000. These guidelines covered change request review, development standards, testing standards, version control, release control, user acceptance, documentation update, user training, and implementation management for the final months of the CMIS and the Part 50 System systems lifetime.

MSHA is currently in compliance with SSP requirements. All major application and GSS SSPs are currently being modified to comply with the SSP reviews and are scheduled to be completed by November 15, 2001. Once these updates are completed for the legacy systems that are being replaced by the MSIS, there will be no significant changes to these systems. Although the MSIS is scheduled for completion of 2002, a delay in that date will certainly not be more than the 3-year update requirement.

Conclusion:
The actions planned by MSHA are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendation. The target date provided for the actions appears reasonable.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.1.4)

Authorize Processing-Certification & Accreditation

Condition:
The CSH and the DOL Manual Series 9 (DLMS-9)--*Information Technology* provide policy and procedural guidance to the DOL agencies regarding certification and accreditation.

However, neither CMIS nor the Part 50 System has been formally certified or accredited since 1994. In addition, neither system is operating with an interim authority to process. Furthermore, actions required for certification and accreditation for CMIS or the Part 50 System have not taken place, as follows:

- "Rules of Behavior" were documented in the SSPs, but have not been signed by users.
- Contingency plans have not been completed or tested.
- The systems are not operating on an interim authority to process.
- In-place safeguards are not operating as intended. For example, we found that passwords to access major applications like the Part 50 System and CMIS are shared among users and management has not acted promptly to address deficiencies.

Cause:
MSHA management has made the decision not to certify or accredit CMIS and the Part 50 System because they do not think that it is cost-beneficial since the two systems will be migrated to a new platform in a couple of years. A top priority for resources has been the MSHA Standardized Information System (MSIS) project, which will migrate CMIS and the Part 50 System into a new client server environment in 2003. However, historically, major system development projects have seldom met projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, MSHA should reconsider their decision, since its sensitive systems and data may be at risk for much longer than two years.

Criteria:
OMB Circular A-130 requires that ". . . A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk or magnitude of harm is high . . . ."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states ". . . Management authorization must be based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by technical evaluation and/or for security evaluation, risk assessment, contingency plan, and signed rules of behavior…Reauthorization should occur prior to a significant change in the system, but at least every three years . . . ."

The NIST FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, explains that the certification process is a technical process that produces a judgment, statement of opinion, and complements the accreditation process.

Accreditation [FIPS 39] is the authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. Accreditation is the official management authorization for operation.

DLMS-9 states that agency heads “. . . are responsible for…issuing Interim Approval to Operate (IATO) under specified conditions to information systems that need to connect to an operational system(s) before full authorization is possible. This may be done in coordination with the CIO on a temporary basis as a facilitating measure to attain full authorization…The IATO may be granted for no more than a one-year period . . . ."

The CSH requires that the Rules of Behavior ". . . should clearly delineate responsibilities and expected behavior of all individuals with access to the General Support System or major application, and must define the consequences of behavior not consistent with the Rules of Behavior . . . It is recommended that the rules contain a signature page for each user to acknowledge receipt . . . .”

Effect:
Without proper certification and accreditation of MSHA's major applications, management cannot be assured that security controls have been designed into its systems as planned, which may leave sensitive data vulnerable to unauthorized access and use.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet authorize processing--certification and accreditation requirements for CMIS and the Part 50 System.

Management Comments:
In order to require users to sign a “Rules of Behavior” statement, the “Rules of Behavior” must be approved by the Unions. The “Rules of Behavior” will be submitted and upon their approval, MSHA users will be asked to sign them.

The Department has re-established the DOL Security Working Group. A workgroup will begin meeting in October of 2001 to develop a C&A process to be included in the Systems Development Life Cycle Management (SDLCM) manual. This process will be used by MSHA to produce an Interim Authorization to process for the CMIS and the Part 50 System. The identification of MSHA’s current risks and threats in the *Vulnerability Report* will be used during that process.

Conclusion:
The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not address action plans or target dates for developing contingency plans for CMIS and the Part 50 System or corrective actions to the sharing of passwords to access the two systems. In addition, MSHA does not provide target dates for planned actions.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.1.5) **System Security Plan**	**Condition:** The CSH and the CSPP provide policy and some procedural guidance to the DOL agencies regarding the development of SSPs. However, the following procedures are not addressed in the above DOL documents: • SSPs should be approved by key affected parties and management. • The summary of the plans should be incorporated into the strategic IRM plan. • The plan should be reviewed periodically and adjusted to reflect current conditions and risks. MSHA has documented an SSP for CMIS and the Part 50 System. The *Major Application Master System Security Plan for MSHA,* dated April 14, 2000, covers the security requirements in place or planned security controls for a total of six MSHA major applications. We confirmed that the *Major Application Master SSP, Major Application SSPs, and MSIS SSP* substantially complied with the CSH and met the majority of the requirements set forth in the NIST SP 800-18 for both CMIS and the Part 50 System. However, MSHA has not fully implemented SSP requirements. In particular, MSHA has not: • Obtained approval of SSPs by all key affected parties and management. • Incorporated a summary of SSP into the strategic IRM plan. • Reviewed the plan periodically and adjusted it to reflect current conditions and risks. • Included all the topics prescribed in NIST Special Publication 800-18, as follows: – A unique identifier for each system/application. – Review of security controls. – Authorize Processing--MSHA has not appointed a designated authorizing management official. – Audit Trails. **Cause:** MSHA has decided not to allocate additional funding and personnel to enhance the legacy systems (CMIS and the Part 50 System) since they will be replaced by the new MSHA Standardized Information System (MSIS). Information security should be practiced throughout all stages of a system's life cycle. The MSIS project is a major system effort and complexities and deadline set backs are inevitable. Although there is a MSIS Project Plan in place, MSHA cannot be assured that MSIS will be fully implemented by its proposed date. As such, MSHA should continue to practice information security and fully implement the SSP requirements for its legacy systems. Another significant impediment to implementin g SSP requirements and information security overall is the absence of top management commitment to information security. While information security may be a concern of the Office of the Assistant Secretary, it is not a high priority. For example, only one person with no staff is assigned to implement the security program for the entire agency and the Office of the Assistant Secretary has not issued any memoranda or other communications promoting information security.

Although the leadership of the Office of Program Evaluation and Information Resources does consider information security to be a priority, they are competing for budgetary resources against programmatic needs more visible to the Office of Assistant Secretary.

Criteria:
The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states "…Each agency shall develop and implement an agency-wide information security program to provide information security for the operations and assets of the agency, including operations and assets provided and managed by another agency . . . ."

OMB Circular A-130 requires Federal agencies to ". . . Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include: Application Rules, Specialized Training, Personnel Security, Contingency Planning, Technical Controls, Information Sharing, and Public Access Controls . . . ."

OMB Bulletin 90-08 states that ". . . The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system . . . ."

FISCAM SP-2 states that (1) ". . . Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities . . .," (2) to help ensure that the plan is complete and supported by the entity as a whole, senior management should obtain agreement from all affected parties in establishing policies for a security program, (3) ". . . To be effective, the policies and plan should be maintained to reflect current conditions . . . Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks, and, therefore, may be ineffective . . . ."

NIST 800-14, *Principles and Practices for Securing Information Technology (IT) Systems*, states that ". . . A security plan should be used to ensure that security is considered during all phases of the IT system life cycle . . . ."

NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that (1) all applications and systems must be covered by SSPs if they are categorized as a "major application" or "general support" system, (2) the purpose of SSPs are to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements, (3) ". . . Authorization is usually supported by a technical evaluation and/or security evaluation, risk assessment, contingency plan, and signed rules of behavior . . . Re-authorization should occur prior to a significant change in the system, but at least every three years . . .," and

(4) in order for the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate.

The CSH states that ". . . One aspect of managing an IT system is the development of a System Security Plan (SSP), which is documentation of the protection afforded the system by technical, managerial, and operational means. In addition, it states that, ". . . A SSP is a living, dynamic document reflecting the current security posture of the IT system. The SSP should be developed during the initial phases of system development and acquisition . . . . The SSP should also be updated on the basis of the subsequent mitigation activity or plan, after a significant system configuration change, or every three years. When the system is decommissioned, the SSP should be updated and stored with system records . . . ."

The CSPP states that all Federal IT systems have some degree of sensitivity and are required to have a SSP and that all DOL systems will have current and effective SSP.

Effect:
Without a detailed SSP, employees may perform inadequate or improper procedures that could, in turn, compromise the security control structure of the organization or place at risk the sensitive data residing within MSHA's systems. In addition, policies, procedures, and guidelines presented within the security plan should be updated periodically or they may not adequately reflect recent modifications within the current working environment of an organization or may not fully support management's overall business and security objectives. Also, without appropriate approval by key affected parties and management of the SSPs, security controls may be overlooked and may not be supported by the entity as a whole. Finally, by not incorporating the summary of SSP into the strategic IRM plan, increases the risk that information management activities may not be carried out in the most efficient, effective, and economical manner.

Recommendations:
We recommend that MSHA:

- Assign appropriate resources and develop and implement action plans to fully meet SSP requirements for CMIS and the Part 50 System.
- Obtain approval of the SSPs from the Office of the Assistant Secretary.

Management Comments:
All major applications and the GSS SSPs are currently being modified to comply with the OCIO SSP reviews and are scheduled to be completed by November 15, 2001. Key affected parties and management will approve SSPs. A summary of the plans will be incorporated into the strategic IRM plan. Once these updates are completed for the legacy systems that are being replaced by the MSIS, there will be no significant changes to these systems. Although the MSIS is scheduled for completion of 2002, a delay in that date will certainly not be more than the 3-year update requirement.

The plans will be reviewed periodically and adjusted to reflect current conditions and risks. The procedure for reviewing and adjusting SSPs will be added to the MSHA Computer Security Program Plan.

	MSHA is in the process of developing the MSIS. The MSIS is a web-based application with an Oracle database. The MSIS integrates and modernizes all of MSHA's legacy mainframe systems. CMIS and the Part 50 System development are frozen and no modifications will be made except those that are legislatively mandated. The first release of an SSP for the MSIS is scheduled for September of 2001. CMIS and the Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the calendar year 2002. The scheduled shutdown for the Honeywell is 11/02 and the IBM is 01/03. **Conclusion:** The actions planned by MSHA are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendation. The target date provided for the actions appears reasonable.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.1) **Personnel Security**	**Condition:** The CSH provides policy and some procedural guidance to the DOL agencies regarding personnel security. MSHA has included some personnel security requirements in the SSPs. For example, MSHA recently documented procedures for employee separation. However, the CSH and MSHA procedures do not specifically require: • All positions to be reviewed for sensitivity level. • Documented job descriptions that accurately reflect assigned duties and responsibilities and segregate duties. • Distinct systems support functions performed by different individuals. • Regularly scheduled vacations and periodic job/shift rotations. • Specific personnel security procedures for hiring and transferringf personnel. MSHA has implemented some personnel security procedures. However, for CMIS and the Part 50 System, MSHA does not: • Identify sensitive functions to be divided among different individuals. • Separate distinct system support functions performed by different individuals. • Require regularly scheduled vacations or job shift rotations. • Have a process for requesting, issuing, and closing user accounts. • Provide background screening for assigned positions prior to granting access. **Cause:** MSHA has not analyzed the costs and other resources and identified action plans necessary to fully implement personnel security. **Criteria:** OMB Circular A-130 requires screening of personnel who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter. FISCAM SD-1 states that management should document job descriptions that clearly describe employee duties and prohibited activities. FISCAM SD-1.1 requires that incompatible duties be identified and policies implemented to segregate these duties. FISCAM SD-4.1 states “. . . The security plan should include policies related to the security aspects of hiring, terminating, and transferring employees and assessing their job performance . . . .” FISCAM SP-1.2 states that ". . . Documented job descriptions should exist that clearly describe employee duties and prohibited activities . . . ." FISCAM SP-4 states that management should include policies related to the security aspects of hiring, terminating and transferring employees and assessing their job performance.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that (1) all positions should be reviewed for sensitivity level, and (2) user access be restricted (least privilege) to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform the job.

Effect:
Without development and implementation of adequate personnel screening requirements, MSHA is exposed to the risk of improper and unauthorized access to its sensitive applications. Improper system access could compromise the efficient working of the systems by misuse, unauthorized modification, viewing of sensitive information, and system disruption.

Recommendation:
We recommend that MSHA identify the personnel security costs and other resources and develop and implement action plans to fully meet personnel security requirements.

Management Comments:
MSHA has no policy in place nor does it anticipate a policy of mandating vacations for employees. This has not been negotiated through the union as a requirement. Although a sound security practice, Federal employees, are only allowed to accrue a certain amount of leave time. Consequently, employees tend to take leave to avoid losing it. As an alternative, "job shift rotations" may be effective in very large organizations with significant depth in each position. MSHA's LAN staff is fairly small, so most staff are already replacing others when they are out.

MSHA’s ISO is currently developing an Exit Policy. This policy will mandate the use of the Separation Clearance form (DOL Form 1-107 - Rev. April 1997). This revision includes a section (1-t) to list system names from which to remove the employee. MSHA exit procedures will instruct supervisors to provide a copy of the completed DOL1-107 to the appropriate LAN Administrator.

The security requirements for contractors working on MSHA systems have been reviewed and appropriate personnel security requirements have been included in each statement of work. In addition, confidentiality agreements are being developed for signature by MSHA employees as well as contractor staff. This will require employee union notification prior to implementation.

The whole issue of appropriate background checks is currently under review in MSHA.

Conclusion:
The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not provide action plans and target dates for implementing all of the personnel security requirements identified in this finding.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.2) **Physical and Environmental Protection**	**Condition:** The CSH provides policy and some procedural guidance to the DOL agencies regarding physical and environment protection controls. However, the CSH and MSHA procedures do not include the following requirements: • Secure unused keys. • Authenticate visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks. • Emergency exit and re-entry of personnel after fire drills. • Change computer room entry codes periodically. • Sign-in and escort visitors into sensitive areas. • Investigate and take remedial action for suspicious access activity. • Review of fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson periodically • Install redundant air-cooling system. • Periodically review electronic power distribution, heating plants, water, sewage, and other utilities for risk of failure. • Provide an uninterruptible power supply or back up generator. • Encrypt data files on laptops. • Store laptops and other portable systems securely. • Protect system from plumbing lines. • Limit viewing of computer monitors by unauthorized personnel. • Control physical access to data transmission lines. Despite the limited procedures, MSHA has regulated access to facilities through the use of guards, identification badges, or entry devices such as key cards. However, based on our interviews, review of documentation, and observations at Arlington, VA and Lakewood, CO sensitive facilities, we found that MSHA does not: • Authorize and log the deposits and withdrawals of tapes and other storage media. • Regularly conduct Management reviews of the list of persons with physical access to sensitive facilities. • Sign in and escort visitors to sensitive areas. • Monitor physical accesses through audit trails and apparent security violations investigated and remedial action taken. • Install fire suppression and prevention devices. • Regularly maintain heating and air-conditioning systems. We also observed the following deficiencies: • The computer room in the Lakewood, CO, facility was observed unlocked and propped open. • "Sensitive" documents printed to the sensitive printer are transferred to lockable mailboxes. These lockable mailboxes contained locks that did not work or were not present. • The Arlington, VA, facility does not have a policy or procedure for storing unused computer room keys; spare keys are stored in the LAN Administrator's locked office in a drawer. • Policies and procedures for a review of fire ignition sources and plumbing dangers have not been developed, or and is not planned in the near future.

- The Arlington, VA, computer facility was observed to be in disarray, which puts the security and physical well being of the equipment at risk.
- Lastly, the data transmission lines for the Arlington, VA, facility are located on each floor in a closet next to the elevator; this closet also houses the electrical and telephone utilities. Hence, building maintenance, telephone maintenance and security employees have access to this closet, leaving the open the risk for tampering.

Cause:
MSHA has not analyzed the costs and other resources and identified action plans necessary to develop and fully implement physical and environmental control requirements.

Criteria:
FISCAM AC-3 requires agencies to establish physical and logical access controls to prevent or detect unauthorized access.

FISCAM AC-3.1 requires ". . . Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment . . . ."

FISCAM SC-2.2 details the policies and procedures that should be in place to prevent potential damage to facilities and interruptions in service and states that ". . . Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. . . . Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages . . . ."

FISCAM AC-4 requires agencies to monitor access, investigate apparent security violations, and take appropriate remedial action details the policies and procedures that should be in place in order to maintain critical audit trails and report unauthorized or unusual activity.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, discusses the physical and environmental security controls that ". . . are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical environmental security program should address the following seven topics--Physical Access Controls, Fire Safety Factors, Failure of Supporting Utilities, Structural Collapse, Plumbing Leaks, Interception of Data, Mobile and Portable Systems. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft . . . ."

DOL Manual Series 9, *Information Technology*, requires agencies to develop procedures ensuring adequate physical security of network assets. The DOL *Security Program Plan Instructions* states that ". . .

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation . . . .”

The CSH requires physical and environmental security controls to be implemented to protect the facility housing system resources, the system resources themselves and the facilities used to support the operation.

Effect:
The lack of clearly defined policy and procedures in place for physical and environment protection controls exposes MSHA to interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Recommendation:
We recommend that MSHA identify the physical and environmental controls costs and other resources and develop and implement action plans necessary to fully meet physical and environmental control requirements.

Management Comments:
Most issues concerning physical and environmental controls are addressed in the MSHA SPP and GSS SSP. Controls at many MSHA facilities are not robust. This is due in part to the fact MSHA leases space and can’t control all of the physical and environmental controls.

MSHA does not have a comprehensive policy for the physical security of IT facilities. A number of the issues addressed as findings in this document were addressed in the MSHA SPP and the GSS SSP; however, they were not codified in policy. This will be addressed in future policy, and will be referenced in the MSHA SPP. These policies will include reference to physical access to IT facilities and control of access; HVAC, water and fire protection; power distribution and protection; key control; access to controlled facilities; and access to data termination points and transmission lines.

The issue of insufficient physical controls on the IRC computer room will be addressed by re-issuing the memorandum dated November 9, 2000. The memo is from the Chief, IRC to the Chief, IRC Systems Operation and Communication Division. IT contains instructions to ensure that the computer room is secured at all times, and to document and report any breaches of the security controls.

MSHA has a draft policy, Appropriate Use of Inspector Laptops. It is due for final review. However, it doesn’t include encryption of data. MSHA hasn’t addressed that issue for laptops. Additionally, MSHA does not have a policy on the control of “sensitive documents” and electronic bulk storage media. These will also be addressed in future policy, and referenced in the MSHA SPP.

Conclusion:
The actions planned by MSHA are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendation. However, MSHA does not provide target dates for completing the planned actions.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.3) **Production, Input/Output Controls**	**Condition:** While DOL and MSHA have policies and some procedures covering production, input/output controls, there are no procedures for: • Transport or mail media or printed output. • Audit trails kept for inventory management. • Physical protection of media storage vault/library. • Process damaged media stored and destroyed. Despite the limited procedures, we found that MSHA has implemented some production, input/output controls, but it has not implemented the following: • Ensuring that only authorized users pick up, receive, or deliver input and output information and media. For example, we found that the Lakewood, CO facility provides mailboxes for sensitive printouts, however, upon observation the locks to the mailboxes were absent or did not work. • Audit trails used for receipt of sensitive inputs/outputs. • Internal/external labeling for sensitivity. • Audit trails for inventory management. • Physical protection of media storage vault/library. • Storage and destruction of damaged media. **Cause:** Prior to 2001 management of information security was decentralized in MSHA, which further inhibited consistent procedures and implementation of information security requirements. However, in January 2001, MSHA centralized the Information Security Office and has begun to analyze security needs and prioritize implementation of various security controls. Also, production, input/output controls are addressed in MSHA's Security Program Plan and the SSP. While MSHA has made many improvements to their security posture since the FY 2000 FISCAM audit, it has not assigned resources or developed action plans to issue procedures and fully implement requirements related to production, input/output controls. **Criteria:** NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology System,* specifically require agencies to develop and implement the following procedures: • Ensuring that only authorized users pick up, receive, or deliver input and output information and media. • Audit trails for receipt of sensitive inputs/outputs. • Procedures and controls used for transporting or mailing media or printed output. • Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary). • Audit trails for inventory management. • Media storage vault or library physical and environmental protection controls and procedures. • Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.

FISCAM, AC-3.4 requires that "... The entity should have procedures in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media . . . ."

The CSH requires that production, input/output controls include measures used to protect information that is input into the system (such as raw data), information that is processed by the system, and the information that is result of processing by the system, such as a report. Examples of controls would be marking, storing, and transmitting sensitive documents; procedures for sanitizing electronic media for reuse or prior to maintenance or repair; and controls for installing an updating software to preclude unintentionally degrading system operation or corruption of data.

Effect:
Without the development and implementation of clearly defined policy and procedures related to production, input/output controls, MSHA runs the risk of loss of input/output information and media and possibly exposing sensitive information to unauthorized users.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet production, input/output control requirements.

Management Comments:
MSHA is in the process of developing the MSHA Standardized Information System (MSIS). The MSIS is a web-based application with an Oracle database. The MSIS integrates and modernizes all of MSHA's legacy mainframe systems. CMIS and the Part 50 System development are frozen and no modifications will be made except those that are legislatively mandated. The first release of an SSP for the MSIS is scheduled for September of 2001. CMIS and the Part 50 System functionality of the MSIS is scheduled to be fully implemented by the end of the calendar year 2002. The scheduled shutdown for the Honeywell is 11/02 and the IBM is 01/03. Consequently, additional resources won't be directed toward changes to the input/output controls on either mainframe. Input/Output controls will be addressed as part of the MSIS implementation.

For management comments regarding audit trails, see the "Audit Trails" section.

Conclusion:
The MSHA response does not address the development of input/output control procedures necessary to bring MSHA into compliance with NIST requirements.

Regarding implementation of input/output controls, MSHA responds that it does not intend to redirect toward changes of input/output controls on either the Honeywell or the IBM mainframe, because those platforms will be shut down in 11/02 and 01/03, respectively. As we stated earlier, the MSIS project is a major system effort and complexities and deadline set backs are inevitable.

	Historically, major system development projects have seldom met projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, the implementation of the input/output controls required by NIST will not occur for potentially several years. MSHA management is aware of the risks, and despite the risks, has decided not to devote any additional resources to input/output controls related to the Honeywell and the IBM mainframe systems.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.4) **Contingency Planning**	**Condition:** The CSH and the CSPP provide policy and procedural guidance to the DOL agencies regarding contingency planning. MSHA has prepared a Y2K Business Continuity and Contingency Plan and tested several major application systems in recent years as a result of the 1995 government shutdown, the 1997 system platform conversion, and 1998 Y2K testing. While progress has been made in implementing contingency planning requirements, MSHA has not: • Completed and tested specific contingency plans for CMIS, the Part 50 System, and the GSS. However, MSHA has prepared a Disaster Recovery and Contingency Plan Outline for those systems. • Provided contingency training, including personnel and data protection and emergency response training to employees. • Provided detailed procedural instructions for restoring operations, including the use of WinFrame software to access remote server or training employees. • Maintained tape inventory or generational data, although back-up logs exist. • Developed disaster and remedial contingency scenarios. • Stored current Y2K Business Continuity and Contingency Plan off-site and made them readily available to employees. The OCIO office recently created a special working group for contingency planning. This working group will include members from each DOL agency and develop detailed templates and procedures for contingency planning applicable to all DOL agencies. **Cause:** MSHA does not plan to devote the necessary resources for contingency planning, because MSHA is reluctant to spend IT resources on contingency planning for its major applications that will be migrated from the Mainframe to a Client-Server Web-based environment as part of the MSIS project. The migration will start in September 2001 and is expected to be completed by the end of 2003. However, historically, major system development projects have seldom met projected implementation dates and, in most cases, more than doubled the original estimated time to implement. Therefore, MSHA should proceed with fully implementing contingency planning requirements for its major applications. **Criteria:** OMB Circular A-130 states that with regards to contingency planning, agencies should ". . . establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support…Experience has demonstrated that testing a contingency plan significantly improves its viability. . . ." NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, ". . . requires that the agency have procedures the will permit a continuation of essential functions if information technology support is interrupted…The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated…General support systems require appropriate emergency, backup and contingency plans . . . .

These plans should be tested regularly to assure the continuity of support…Also, these plans should be known to users and coordinated with their plans for applications . . . .”

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that “. . . an organization should test and revise the contingency plan. A contingency plan should be tested periodically . . . .” It also indicates the functional steps that an organization should employ when preparing for contingencies and disasters. These steps are (1) develop a business plan, (2) identify resources (3) develop scenarios, (4) develop strategies, and (5) test and revise the plan.

FISCAM, SC-1.3 states that “. . . In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed . . . .”

FISCAM, SC-2.1 states that “. . . Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions . . . ."

FISCAM, SC-3.1 states that “. . . Contingency plans should be documented, agreed on by both user and data processing departments, and communicated to affected staff…Staff should be trained in and aware of their responsibilities in preventing mitigating and responding to emergency situations . . . . Training sessions should be held at least once a year and whenever changes to emergency plans are made . . . [The plan] should identify and provide information on:

- Supporting resources that will be needed,
- Roles and responsibilities of those who will be involved in recovery activities,
- Arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, if needed,
- Off-site storage location for backup files, and
- Procedures for restoring critical applications and their order in the restoration process.” “Multiple copies of the contingency plan should be available with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable . . . .”

DLMS-9 requires that a contingency plan/disaster recovery plan for all information systems within a DOL agency must be completed prior to approval of SSPs.

Effect:

The absence of formal contingency plans and periodic testing of those documents could result in significant delays in restoring operations in the event of system failures.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet contingency planning requirements for CMIS, the Part 50 System, and MSHA's GSS.

Management Comments:
MSHA plans to complete all components of the MSHA Computer Security Handbook in FY 2002. One of the components of the handbook is the MSHA Contingency Plan. The phases of the contingency plan development are:

- Preplanning and Strategy Development Phase
- Planning Phase (Writing the Plan)
  - Plan Design Basics
  - Seven-Step Contingency Planning Process
- Post Planning Phase
  - Training on the Plan
  - Testing and Exercising the Plan

Conclusion:
MSHA does not provided target dates for the implementation of the contingency planning procedures planned.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.5) **Hardware and System Software Maintenance**	**Condition:** The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding hardware and system software maintenance. MSHA's *Administrative Policy and Procedures Manual for Information Technology Resources* (APPM) also provides MSHA with additional guidance in this area. However, none of the documents provide the following procedures: • Document detailed system specifications and complete management review. • Define type of test data to be used. • Set default settings of security features in the most restrictive mode. • Provide software distribution implementation orders including effective date provided to all locations. • Establish Version Control. • Document and obtain management approval for emergency change procedures, either prior to the change or after the fact. • Update contingency plans and other associated documentation updated to reflect system changes. We also found that MSHA has not implemented procedures to: • Place restrictions on who performs maintenance and repair activities. • Restrict access to all program libraries. • Develop on-site and off-site maintenance procedures. • Implement an impact analysis to determine the effect of proposed changes on the existing security controls, including the required training needed to implement the control. • Use software change request forms to document request and related approvals. • Review the distributio n and implementation of new or revised software. • Provide software distribution implementation orders including effective date provided to all locations. • Document and obtain management approval for emergency change procedures. **Cause:** MSHA has not assigned resources or developed action plans to fully implement hardware/system software maintenance requirements. **Criteria:** The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that, ". . .The head of each agency [should]…(A) adequately ensure the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets . . . ." FISCAM CC-1.2 states that ". . . Allowing employees to use their own software, or ever use diskettes for data storage that have been used elsewhere, increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software . . . ."

	FISCAM CC-2.1 states that “. . . Once a change has been authorized, it should be written into the program code and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of procedures or standards for prioritizing, scheduling, testing, and approving changes . . . .” FISCAM CC-2.3 states that “. . . Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software . . . . Once a modified software has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it . . . .” FISCAM CC-3.2 states that ". . . Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. Separate libraries should be established for (1) program development and maintenance, (2) user testing, and (3) production. Also, controlled copies of the source versions of all programs (the code created by programmers) should be separately maintained and protected from unauthorized access. If unauthorized modifications are suspected of a production program, the source code can be recompiles to determine what has been changed . . . .” FISCAM CC-3.3 states that “. . . The movement of programs and data among libraries should be controlled by an organization segment that is independent of both the user and the programming staff . . . .” FISCAM SC-2.1 states that “. . . Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions . . . .” FISCAM SS-3.1 states that system software changes are authorized, tested, and approved before implementation. FISCAM SS-3.2 states that “. . . When possible, the installation of system software changes and new versions or products should be scheduled to minimize the impact on data processing operations, and an advance notice should be provided to system software users . . . .” DLMS-9 establishes policy and procedure governing the authorized acquisition, reproduction and distribution or transmission of licensed and copyrighted computer software in DOL. The CSH requires that SSPs address hardware and system software maintenance controls over (1) servicing equipment on-site and off-site (2) documenting changes and approvals, (3) version control process, (4) distribution and implementation of new or revised software.

Effect:
The lack of effective hardware and system software maintenance procedures and implementation could pose security vulnerability through:

- Inaccurate or missing record of changes in software and hardware.
- Improper or unauthorized changes to hardware and system software.
- Incomplete impact analysis of changes on the security configuration of the system.
- Lack of a medium for MSHA personnel to consistently communicate all baseline changes within and outside the agency.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet hardware and system software maintenance requirements.

Management Comments:
The issue of hardware maintenance is addressed in the MSHA SPP. PCs are not locked. Therefore, it is technically possible for any member of the staff to access a PC and conduct hardware maintenance. However, this would be most unusual. Most maintenance operations on a PC running Windows NT® require administrator privileges. The privileges are assigned, for the most part, to IT staff who perform Maintenance. Very few end users have this level of privilege assigned.

MSHA has recently approved and implemented a Configuration Management Plan. This plan provides for a detailed process on the modification, update, or upgrade to all software running on the system, to include operating systems, and provides for version control. The plan considers potential impact to the enterprise as a component of determining whether software can be installed. The plan also addressed the issue of software distribution. System Change Request forms are used. Emergency procedures are in place for critical updates, e.g., virus updates.

Conclusion:
Based on the MSHA SPP and implementation of the Configuration Management Plan, MSHA meets the intent of our recommendation.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.6) **Data Integrity**	**Condition:** The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding data integrity. The MSHA GSS SSP also provide MSHA with additional guidance in this area. However, the following procedures are not covered by DOL or MSHA: • Automate virus scans. • Use reconciliation routines for applications (i.e., checksums, hash totals, record counts). • Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions. • Investigate inappropriate or unusual activity and take appropriate actions. • Review intrusion detection reports routinely and handle suspected incidents accordingly. • Use message authentication used. MSHA has implemented some data integrity requirements. However, the following procedures have not been implemented: • Automate virus scans. • Use reconciliation routines for applications (i.e., checksums, hash totals, record counts) • Execute procedures to determine compliance with password policies. • Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions. • Investigate inappropriate or unusual activity and take appropriate actions. • Review intrusion detection reports routinely and handle suspected incidents accordingly. • Use system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attack. • Perform penetration testing performed. • Use message authentication. **Cause:** MSHA has not assigned resources or developed action plans to fully implement data integrity requirements. **Criteria:** The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA), states that, “. . . The head of each agency . . . (A) adequately ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets; (B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency . . . ." OMB Circular No A-130 states “. . . ‘adequate security' means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

This includes assuring that systems and applications used by the agency operate effectively

and provide appropriate confidentiality, integrity, availability, through the use of cost-effective management, personnel, operational and technical controls . . . .”

FISCAM SS-2.2 states that inappropriate or unusual activity should be investigated and appropriate actions taken details the policies and procedures that should be taken when inappropriate or unusual activity occur which may contribute to data integrity issues.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, is a comprehensive document that details the policies that should be enforced in regards to securing information technology systems and promoting data integrity.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, advises that the determination of adequate controls over data integrity requires answers to whether integrity verification programs are used by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing to determine whether the access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual) and whether system performance monitoring is used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes.

APPM, *Information Technology Resources*, provides policies and procedures requiring a data requirements document as part of their System Development Life Cycle to promote data integrity and increase the awareness of controls and security in automated information systems.

Effect:
The lack of effective data integrity controls could pose security vulnerability through:

- Inaccurate or missing data resulting from unauthorized destruction or tampering of electronic files and records.
- Access to proprietary or sensitive data by unauthorized personnel.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet data integrity requirements.

Management Comments:
MSHA has recently completed policy that will mandate the use of automated virus scanning on all systems connected to the network. That policy will be implemented shortly.

MSHA has not yet developed definitions for sensitivity based on individual levels, nor does MSHA have the tools in place to ensure data integrity.

	MSHA does not anticipate possible implementation of these tools before FY 2003. However, in the MSHA SPP, MSHA has defined the requirements for determining how integrity will be achieved. MSHA has budgeted for the installation and operation of an Intrusion Detection System (IDS) for FY 2002. Policies and procedures will be developed for operation of the IDS. This policy will be placed in the Technical Operations Manual. MSHA has implemented both a process for validating compliance with password policies, and for performing network performance monitoring; however, neither process has been formalized with a policy. The password validation policy will be addressed in the MSHA SPP, and the network performance policy will be addressed in the Network Operations Manual. MSHA networks have been subjected to penetration testing for the last two fiscal years. However, policy requiring penetration testing is scheduled to be developed and will be addressed in the MSHA SPP. **Conclusion:** The actions planned by MSHA are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendation. The target dates provided for the actions appear reasonable.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.7) **Documentation**	**Condition:** The CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding documentation requirements. MSHA's SSPs for its GSS and its Major Applications also provide MSHA with additional guidance in this area. However, there are no DOL or MSHA requiring the following: • Standard operating procedures exist for all the topic areas covered in the NIST Self-Assessment Guide. • Emergency procedures. • Backup procedures. • Procedures restricting access to software documentation related to the system security features to the system administrator and system security officer. MSHA has implemented some of the documentation requirements. However, MSHA has not completed the following documentation: • Emergency procedures. • Contingency plans. • Certification and accreditation documents and statements authorizing the systems to process. In addition, MSHA has not restricted access to software documentation related to system security features to the system administrator and system security officer. **Cause:** Information Security Personnel are in the process of enhancing current security policy, procedures and other applicable security documentation. However, MSHA has not assigned resources or developed action plans to fully implement documentation requirements. **Criteria:** OMB Circular A-130, regarding how agencies will ensure security in information systems, states that agencies must ". . . incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning . . . ." NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* states that ". . . Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures . . . ." NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* states that ". . . Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently . . . ."

Effect:
Lack of documentation can lead to difficulty in supporting and enhancing MSHA's systems in the future. The lack of complete documentation could also lead to incomplete security policy and procedure functionality being followed, thus leaving the system vulnerable to threats. In addition, if updated and consistent security documentation is not available for access, users may involuntarily compromise MSHA's security practices, thus leaving its systems unsecured and susceptible to various vulnerabilities and threats, both internal and external.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet documentation requirements.

Management Comments:
For management comments regarding contingency plans – See Section 4.2.4, Contingency Planning.

For management comments regarding certification and accreditation – See Section 4.1.4, Certification and Accreditation.

Emergency and backup policy and procedures are scheduled to be written and included in the Technical Operations Handbook.

Policy to restrict access to software documentation related to system security features is scheduled to be written and included in the Technical Operations Handbook.

Conclusion:
The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not provided target dates for the actions planned. In addition, MSHA does not fully respond to the documentation issues related to contingency plans and certification and accreditation, as discussed under the "Conclusion" sections in "Contingency Planning" and "Authorize Processing--Certification & Accreditation" sections of this report.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.8) **Security Awareness, Training, and Education**	**Condition:** The CSH provides policy and procedural guidance to the DOL agencies regarding security awareness, training, and education. The CSH is available to all DOL employees through the LaborNet intranet. While MSHA has implemented most of the security awareness, training, and education requirements, it does not currently have a comprehensive security training program. Their current training and security awareness program includes awareness and basic training, but not role-based training or education. In addition, MSHA has not documented and monitored employee training and professional development. **Cause:** For the last two years, MSHA has been in the process of implementing a significant number of security initiatives to meet all DOL and statutory requirements. Consequently, security awareness, training, and education was not a high priority and MSHA did not allocate the resources to fully develop and implement appropriate procedures. In the FISCAM Audit of FY 2000, MSHA management recognized that they were deficient in implementing policy and procedures for the security awareness program. MSHA plans to implement specific training classes for technical persons and managers. While MSHA has plans to improve security awareness, training, and education, it has not assigned resources or developed action plans to fully implement the requirements in this area. **Criteria:** The Computer Security Act of 1987 states that ". . . each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of that agency . . . ." U.S. Office of Personnel Management Regulation requires that the head of each agency identify employees responsible for the management or use of computer systems that process sensitive information and provide initial and periodic refresher security awareness training specific to each of the following groups: executives, program and functional managers, and IRM, security, and audit personnel. OMB Circular A130 states that training should be provided to "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system. In addition, this circular requires that agencies ". . . Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system . . . Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system . . . ."

FISCAM SP-4.2 states "... management should ensure that employees have the expertise to carry out their information security responsibilities. To accomplish this, the security program should include:

- Job descriptions
- Periodically reassessing the adequacy of employee's skills
- Annual training requirements and professional development programs
- Monitoring employee training and professional development accomplishments . . . ."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "... A set of rules of behavior must be established for each system. . . . The rules of behavior should be made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt . . . ."

The CSH requires rules of behavior for all systems. The CSH states that the rules of behavior should clearly delineate responsibilities and expected behavior of all individual with access to each agency system and must define the consequences of behavior not consistent with the rules of behavior.

Effect:
Without taking the necessary steps to provide adequate security training, and education and to document and monitor that training and education, the agency can not be assured that all individuals involved in the use, design, management, acquisition, maintenance or operation are aware of their security responsibilities or how to fulfill their security responsibilities. For example, the costly recovery efforts required to eliminate the "I Love You" virus, in general, might have been mitigated to a greater extent if employees were more knowledgeable about what to do regarding unsolicited emails.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet security awareness, training, and education requirements.

Management Comments:
MSHA's detailed Security Work Plan includes completion of all components of the MSHA Computer Security Handbook in FY 2001 and 2002. One of the components of the handbook is the "Computer Security Awareness and Training Guide." Along with policies and procedures, the major components of the guide include:

- Roles and Responsibilities
- Training Requirements
- Computer Security Continuum:
  - Education
  - Awareness
  - Training
- Computer Security Training Program
- Training Evaluation

	Conclusion: The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not address documentation and monitoring of employee training and professional development.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.9) **Incident Response Capability**	**Condition:** The CSH provides policy and some procedural guidance to the DOL agencies regarding incident response capability. However, the CSH and MSHA procedures do not specifically require: • Training personnel to recognize and handle incidents. • Modifying incident responsibility capability procedures and control techniques after an incident takes place. • Sharing incident information and common vulnerabilities or threats with other organizations with interconnected systems. • Reporting incidents, vulnerabilities, and threats to Federal Computer Incident Response Capability (FedCIRC) and other Federal and local law authorities. Despite the limited procedures, MSHA has established and maintained a formal incident response capability and process and does monitor and track incidents until resolution. In addition, management recently developed procedures to expedite helpdesk calls deemed to be potential computer security incidents and has recently hired a contractor to evaluate and update the helpdesk Escalation Procedures for Computer Security Incidents. We also found that users in the field were notified via email of incidents. However, MSHA has not: • Provided training to recognize and handle incidents. • Established a process to modify incident handling procedures and control techniques after an incident occurs. • Shared and reported related information with other organizations (e.g., interconnected systems, FedCIRC, and other Federal and local law authorities). • Established an official Computer Security Incident Response Team recognized by the DOL Office of the Chief Information Officer (OCIO). Other deficiencies were noted, as follows: • Although MSHA has a significant number of remote lap top and field office users, McAfee virus software updates are not distributed to remote users and users in the field offices. • LAN Administrators do not monitor the system for possible security incidents. • Intrusion attempts and abnormalities logged by the intrusion detection software are not monitored on a regular basis. • MSHA security personnel did not complete and submit a written Incident Report or Follow-up Report through the appropriate reporting chain concerning the “I Love You” virus incident. • The recent type 2 security incident the "I Love You" virus that occurred in MSHA and elsewhere throughout DOL was identified and reported to a help desk. However, the subsequent reporting chain remains undocumented and resolution was not properly documented. The “I Love You” virus spread via email and infected several PCs, although CMIS and the Part 50 System were not affected. The MSHA Information Security Office did not have a written Incident Report or Follow-up Report on file, nor did the OCIO have a record of the MSHA security incident in their Department-wide incident log.

Cause:
For the last two years, MSHA has been in the process of implementing a significant number of security initiatives to meet all DOL and statutory requirements. Consequently, incident response capability was not a high priority and MSHA has not developed any action plans or assigned resources to develop and implement procedures to meet incident response capability requirements.

Criteria:
The FY 2001 Defense Authorization Act, *Government Information Security Reform Act (GISRA)* states agencies must have "*. . .* procedures for detecting, reporting, and responding to security incidents, including…notifying and consulting with law enforcement officials and other offices and authorities . . . ."

OMB Circular A-130 requires that agencies establish formal incident response mechanisms and make system users aware of these mechanisms and how to use them. The circular further states that **"**. . . To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide . . . ."

FISCAM SP-3.4 requires ". . . agencies to establish formal incident response mechanisms and to make system users aware of these mechanisms and how to use them . . . ."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* states that ". . . when faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident . . . ."

DLMS-9 and CSPP require all DOL agencies to train users on incident reporting, establish and maintain an ad hoc CSIRT and report all incidents appropriately.

The DOL Computer Security Handbook (CSH), Chapter 5, requires MSHA to assign the appropriate resources to support the Computer Incident Reporting and Response Program. The CSH specifically requires MSHA to:

- Develop and implement procedures to ensure timely detection and reporting of actual or suspected violations.
- Assign an agency point of contact for computer security matters to ensure a response is available 24 hours a day, 7 days a week for computer incidents
- Designate the members of the Computer Security Incident Response Team (CSIRT) and forward their names to the OCIO.
- Provide the agency CSIRT training on the agency's computer security chain and recognizing and responding to computer security incidents and anomalies.
- Complete a written Initial Incident Report for all Type 2 and Type 3 incidents and submit to the OCIO.

Effect:
Without properly written, distributed, and executed incident reporting procedures, the risk that computer viruses can cause costly resource intensive resolution increases. In addition, without adequate and proper training, MSHA is susceptible to incorrectly responding to and/or mishandling reported incidents. Improperly handling a reported incident could compromise the information systems security to additional threats or result in not resolving the threat in the most cost-effective method and/or in a timely manner.

Without adequate and proper training, MSHA is susceptible to incorrectly responding to and/or mishandling reported incidents. Improperly handling a reported incident could compromise the information systems security to additional threats or result in not resolving the threat in the most cost-effective method and/or in a timely manner. If MSHA does not share incident information and common vulnerabilities and threats with other interconnected systems, multiple systems may be susceptible from a single threat source.

Recommendation:
We recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet incident response capability requirements.

Management Comments:
MSHA's detailed Security Work Plan includes completion of all components of the MSHA Computer Security Handbook in FY 2001 and 2002. One of the components of the handbook is the "Incident Response and Reporting Guide." Along with policies and procedures, the major components of the guide include:

- Roles and Responsibilities
- Computer Security Incident General Procedures:
  - Planning
  - Implementing and Monitoring of Intrusion Detection
  - Reporting Procedures
  - Computer Security Incident Response Teams
  - Incident Log
  - Investigating Incidents
  - Recovery Procedures
- MSHA Detailed Technical Incident Response Procedures

Conclusion:
The actions planned by MSHA are partially responsive to the issues identified. However, MSHA does not specifically address all the development and implementation of incident response capability procedures identified in the finding. For example, development and implementation of procedures related to training personnel to recognize and handle incidents and sharing incident information with other organizations is not specifically addressed.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.1) **Identification and Authentication**	**Condition:** The CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding identification and authentication requirements. MSHA has also provided guidance in this area. However, DOL or MSHA procedures do not require the following: • Establish the system capability to correlate actions to users. • System owners periodically review access authorization listings to determine whether they remain appropriate. MSHA has implemented many of the identification and authentication requirements. However, the following requirements have not been implemented: • Establish the system capability to correlate actions to users. • System owners periodically review access authorization listings to determine whether they remain appropriate. • Prohibit access scripts with embedded passwords. • Limit the number of invalid access attempts that may occur for a given user. • Passwords are not shared by multiple users. • Terminals, workstations, and networked personal computers are not left unattended when the user ID and password are logged in. **Cause:** MSHA has not assigned resources or developed action plans to fully implement identification and authentication requirements. **Criteria:** OMB Circular A-130 states that ". . . individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job . . . ." FISCAM AC-2.1 states that ". . . the computer resource owner should identify the specific user or class users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties . . . The owner should also identify the nature and extent of access to each resource that is available to each user . . . . " In general, users may be assigned one or more of the following types of access to specific computer resources: read, update, delete, merge, and/or execute. FISCAMAC-2.2 states that ". . . Emergency and temporary access authorization is controlled . . . ." Emergency and temporary access authorizations should be ". . . documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period . . . ." The audit techniques include ". . . review of pertinent policies and procedures, compare a selection of both expired and active temporary and emergency authorizations with a system-generated list of authorized users, and determine the appropriateness of access documentation and

approvals and the timeliness of terminating access authorization when no longer needed . . . . ”

FISCAM AC-3.2 states that “. . . Identification is the process of distinguishing one user from all others, usually through the use of user IDs. User IDs are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. Typical controls for protecting the confidentiality of passwords include the following: password selection is controlled by the assigned user, passwords are changed periodically, about every 30 to 90 days, passwords are not displayed when they are entered, minimum character length, at least 6 characters, is set for the passwords so that they cannot be easily guessed, use of names, words, or old passwords within six generations is prohibited, while use of alphanumeric passwords should be encourages, vendor-supplied passwords are replaced immediately upon implementation of a new system, and individual users are uniquely identified rather than having users within a group share that same ID or password . . . .”

FISCAM AC-3.2 also states that “. . . to help ensure that passwords cannot be guessed, attempted to log on the systems with invalid passwords should be limited. Typically, potential users are allowed three or four attempts to log on . . . .” Lastly, another technique for reducing the risk of password disclosure is encrypting the password file. Encryption further reduces the risk that the password file could be accessed and read by unauthorized individuals.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that “. . . identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system . . . .”

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that ". . . Passwords should be changed periodically . . . If passwords are used for authentication, organizations should specify Required Attributes. Secure password attributes such as a minimum length of six, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required . . . .”

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that “. . . Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability . . . .” NIST 800-12 provides ways of improving password security: password generators, limits on log-in attempts, password attributes (e.g., passwords with a certain minimum length, use of special characters, picking passwords that are not in an on-line dictionary), periodic changing of passwords, and technical protection of the password file (e.g., one-way encryption).

Federal Information Processing Standards Publication 186-1 lays out a standard in the encryption algorithm.

The CSH requires the analysis of identification and authentication controls in the development of SSPs.

Effect:
MSHA password management involves the techniques and mechanisms used to adequately protect CMIS and the Part 50 System and its user passwords from disclosure to unauthorized individuals. Passwords are the primary security mechanism used to authenticate a user in order to protect user accounts and prevent access to information from unauthorized individuals. Good password management increases the protection of user passwords, thus enhancing the security of the system. Poor password management can create holes in the system security. Disgruntled employees, terminated employees, and hackers pose major threats to any weaknesses found in password management, and if exploited, the systems may be at risk.

Recommendations:
We recommend that MSHA take immediate action to regularly pull the current passwords from all servers including the primary domain server, the web servers, and DNS servers as well as any other systems considered integral to operations. These passwords should be checked for strength with automated password checking software called password crackers.

We also recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet identification and authentication requirements.

Management Comments:
MSHA's 2003 Security Crosscut Decision Paper includes a provision for implementing a stronger identification and authentication process. A review of the Application Database Managers' user group was conducted. SAAR forms were prepared and authorized for all system users to ensure that only valid, authorized users have access to the system. Users without the requisite authorizations no longer have access to the system.

The use of generic user IDs and passwords is not permitted on MSHA's LAN. Each user has a unique ID and the policy states that users are not to share IDs. It is not the policy on the LAN to automatically log off a user after a period of inactivity, nor does MSHA plan to institute such a policy. However, MSHA's policy is to lock users out automatically after 15 minutes of inactivity on the LAN. Users must re-enter their passwords to resume the network session. Additionally, LAN users have been instructed to log off their computers when they leave for the day.

Conclusion:
The actions planned and taken by MSHA are partially responsive to the issues identified. However, MSHA does not fully address the development of procedures identified in this finding to bring MSHA into compliance with the NIST requirements.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.2) **Logical Access Controls**	**Condition:** The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding logical access control requirements. In addition, MSHA's *Software Load and Standard Architecture Design, Configuration, and Implementation Plan* has established additional policies and procedures regarding logical access controls over MSHA data. However, the following procedures are not covered by any of the above documents: • Establish security controls detect unauthorized access attempts. • Implement access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion. • Restrict access to security software to security administrators. • Monitor inactive users' accounts and remove when not needed. • Use internal security labels (naming conventions) to control access to specific information types or files. • Disable insecure protocols (e.g., UDP, ftp). • Maintain and review network activity logs. • Monitor dial-in access. • Authorize and monitor guest and anonymous accounts. MSHA has implemented many of the logical access controls requirements. However, the following requirements have not been implemented: • Implement access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion. • Restrict access to security software to security administrators. • Use internal security labels (naming conventions) to control access to specific information types or files. • Monitor dial-in access. **Cause:** MSHA has not assigned resources or developed action plans to fully implement logical access control requirements. **Criteria:** OMB Circular A-130 states that ". . . individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job . . . ." NIST SP 800-18 states that ". . . Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users . . . ."

FISCAM AC-3.2 states that "... to ensure that access controls are uniformly administered, the security management function should implement and maintain logical access controls based upon authorizations from appropriate levels within the entity . . . ."

FISCAM SD-2.1 indicates that physical and logical controls should be established. It further states that ". . . both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities . . . ."

The CSH defines logical access controls as ". . . system-based mechanisms that provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make . . . ." The CSH states that logical controls should authorize or restrict the activities of users and system personnel within the GSS, permit only authorized access to or within the GSS, restrict users to authorized transactions and functions, and detect unauthorized activities.

Effect:
On-line systems are dependent on telecommunications access to the computer systems (local and/or central) that provide service. Exposure to the malfunctions of hardware, software, or communications can impair the adequacy of service or the accessibility of information. While protecting the computer systems and supporting environments is important, the physical and logical networks must also be protected.

Uncontrolled access to public networks, such as the Internet, increases the risk of systems not being available when required and threatens the safety of internal information assets.

The complexity of controlling access is made more difficult by decentralization of computing capabilities and the diversity of communication paths. Insufficient security networks and inadequate system controls increase the risk of unauthorized access. Without software security (which may be part of the operating system, or separate software or a combination of both) there would be an inability to validate identification of the user, access device, and permissible transactions and would increase the risk of unauthorized access and system misuse.

Recommendations:
We recommend that MSHA take the following actions as soon as possible:

- Install and independently test an intrusion detection system and a central logging system.
- Update and implement policies and procedures regarding the monitoring of the MSHA network to include information specific to the intrusion detection and the central logging system.
- Require network administrators to regularly scan the network for vulnerabilities using automated tools.
- Enlist an independent security team that specializes in identifying vulnerabilities whenever new servers or applications are implemented.

We also recommend that MSHA assign appropriate resources and develop and implement action plans to fully meet logical access controls.

Management Comments:
MSHA has budgeted for the installation and operation of an Intrusion Detection System (IDS) for FY 2002.

An Information Security (INFOSEC) engineer has been contracted to support MSHA. Network monitoring through the Information Security Office (ISO) has already been implemented, with positive results. A procedure defining which inspection tools will be run, and when, is under development.

The MSHA System User Rules of Behavior document will be updated to restrict system administrators from installing or using any security-oriented applications, to include sniffers, password crackers, etc. Only security staff will be authorized to use these tools.

As noted in the "Personnel Security" section above, MSHA's Human Resources Division is developing a policy and procedures for exiting MSHA employees. This policy will mandate the use of the Separation Clearance form (DOL Form 1-107 - Rev. April 1997). This revision includes a section (1-t) to list system names from which to remove the employee. MSHA exiting procedures will include instructions for each employee's supervisor to provide a copy of the completed DOL1-107 to the appropriate LAN Administrator.

MSHA is already using Windows NT® and the NTFS file system to provide discretionary access control on the network. MSHA does not anticipate the use of naming conventions for documents to further secure documentation. Windows NT® provides a sufficient degree of granularity for controlling access to documents.

The use of generic user IDS and passwords is not permitted on MSHA's LAN. It is not the policy on the LAN to automatically log off a user after a period of inactivity, nor does MSHA plan to institute such a policy. However, MSHA's policy is to lock users out automatically after 15 minutes of inactivity on the LAN. Users must re-enter their passwords to resume the network session. Additionally, LAN users have been instructed to log off their computers when they leave for the day.

MSHA's program for dial-up connectivity has been poorly managed. A policy controlling how the dial-up program will be managed will be developed. This policy will include guidance on monitoring dial-in logs. The policy will be developed and filed in the Network Operations Manual. MSHA has no plans to authorize the guest or anonymous accounts.

Controls on the MSHA ftp server will be modified to provide an appropriate level of security. Other instances of the use of the ftp and UDP protocols will be disabled where appropriate.

Generic IDs and passwords are permitted on the Bull system. On the Bull system, users are logged off of the system after a relatively short period of inactivity.

	User-ID and password combinations on the SunGard mainframe restrict user access to the major application and directories they have logical access to - via mainframe RACF security software and the IBM Operating System. Additionally, each major application has its own permissions to those files and directories unique to that application's accesses. On the SunGard, a single user-ID may access more than one major application. User-IDs are granted to individual users and restricted by RACF. **Conclusion:** The actions planned and taken by MSHA are partially responsive to the issues identified. However, MSHA does not provide target dates for the development and implementation of the planned procedures.

NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.3)

Audit Trails

Condition:
The CSH and DLMS-9 provide policy guidance to the DOL agencies regarding audit trail requirements. However, neither DOL nor MSHA provides any specific procedural guidance in this area.

Despite the lack of procedures, MSHA has implemented many of the audit trail requirements. However, the following procedures have not been implemented:

- Audit trails can support after-the-fact investigations of how, when, and why normal operations ceased.
- Strictly control access to online audit logs.
- Ensure separation of duties exist between security personnel who administer the access control function and those who administer the audit trail.
- Review audit trails frequently.
- Distribute audit trail regularly to appropriate managers.
- Audit reports should be reviewed regularly by System Security Officer.

Cause:
MSHA has not assigned resources or developed action plans to fully implement audit trail requirements.

Criteria:
The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that the head of each agency shall develop and implement an agency-wide information security program to include "procedures for **detecting**, reporting, and responding to security incidents . . ." (emphasis added).

FISCAM AC-4 states that ". . . security software generally provides a means of determining the source of a transaction of an attempted transaction and of monitoring users' activities (the audit trail). However, to be effective (1) this feature should be activated to maintain critical audit trails and report unauthorized or unusual activity and (2) managers should review and take action on these reports . . . ."

NIST Special Publication 800-18*: Guide for Developing Security Plans for Information Technology Systems*, states that agencies should have "…Audit trails maintain a record of system activity by system or application processes and by user activity . . . [and should consider whether] . . . (1) the audit trail support[s] after-the-fact investigations of how, when, and why normal operations ceased . . .; (2) The audit trail provide[s] accountability by providing a trace of user actions . . .; (3) access to online audit logs [is] strictly controlled . . .; (4) . . . separation of duties between security personnel who administer the access control function and those who administer the audit trail [exists]; and (5) how frequently audit trails are reviewed and whether there are review guidelines . . . ."

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* states that ". . . audit trails maintain a record of system activity by system or application processes by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification . . . .”

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that “. . . an audit trail should include sufficient information to establish what events occurred and who (or what) caused them . . . .” An event record should specify what event occurred, the User ID associated with the event, the program or command used to initiate the event, and the result.

The CSH states that “. . .audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. Audit trails provide a means to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis . . . .” Audit trails should provide accountability to users for their actions such as type of event, when the event occurred, the user ID associated with the event, and the program and command used to initiate the event.

Effect:
During the course of penetration testing multiple password guessing attempts on users accounts within the MSHA NT Domain resulted in locked out accounts. When the accounts were locked out MSHA LAN Administrator could not positively identify the cause of the attacks. It was only after MSHA LAN Administrators identified that accounts were locked out that the administrators enabled auditing of system events on the NT Domain systems. Later, MSHA LAN Administrators determined the penetration tests caused the lockouts.

Audit trails document the activities by authorized and unauthorized individuals on the system. When there is a lack of auditing on a system, user activities on the system cannot be recorded or tracked and the system is highly vulnerable to external or internal attacks without any notice to the administrator or security personnel. If auditing has been invoked, but the audit reports are not generated and reviewed on a regular basis, the system is also vulnerable to attacks because previous attacks may go undetected.

Logs not backed up to tape and stored in a central logging facility are vulnerable to manipulation. For example, if a server is compromised, its audit log files can be deleted or falsified. In addition, audit logs stored on the local system are susceptible to manipulation and will not withstand scrutiny under the eyes of the law should there be question in a court case.

Recommendation:
We also recommend that MSHA develop action plans and assign resources to fully implement all remaining audit trail requirements.

Management Comments:
MSHA is still developing policies and procedures addressing a number of security issues. While an audit program has been implemented, policies have not yet been developed. Auditing has been addressed in the MSHA Security Program Plan, and will be codified as policy.

	The issue of separation of duties is addressed in the MSHA SPP. MSHA has not yet divided responsibilities between system administrators and the Information Security Officer. Guidance concerning appropriate division of responsibility will be addressed in forthcoming policy. **Conclusion:** The actions planned and taken by MSHA are partially responsive to the issues identified. However, MSHA does not provide target dates for the development and implementation of the planned procedures.

ACRONYMS

APPM	Administrative Policy and Procedures Manual
CIO	Chief Information Officer
CMIS	Coal Management Information System
COBOL	Common Business Oriented Language
CSPP	Cyber Security Program Plan
CSH	Computer Security Handbook
CSIRT	Computer Security Incident Response Team
DLMS	DOL Manual Series
DNS	Domain Name Server
DOL	Department of Labor
FedCIRC	Federal Computer Incident Response Capability
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Systems Controls Audit Manual
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSS	General Support System
HVAC	Heating, Ventilation and Air Conditioning
IATO	Interim Approval to Operate
IDS	Intrusion Detection System
IG	Inspector General
INFOSEC	Information Security
IRM	Investment Resource Management
ISO	Information Security Office
IT	Information Technology
LAN	Local Area Network
MSHA	Mine Safety and Health Administration
MSIS	MSHA Standardized Information System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
Part 50 System	MSHA Part 50 System
PDD	Presidential Decision Directive
PwC	PricewaterhouseCoopers, LLP
SDLC	Systems Development Life Cycle
SDLCM	Systems Development and Life Cycle Management Manual
SSP	System Security Plan
ST&E	Security Testing and Evaluation
TFAR	Tentative Finding and Recommendations
WAN	Wide Area Network

Appendix A

MANAGEMENT RESPONSE TO THE DRAFT REPORT

MSHA's Response to the GISRA Draft Audit Report No. 23-01-011-06-001

NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.1)
Risk Management

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.2)
Review of Security Controls

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.3)
Life Cycle

MSHA Response:

The DOL CSH states that "The SSP should be updated on the basis of the subsequent mitigation activity or plan, after a significant system configuration change or every three years."

MSHA completed a General Support System Security Plan and a Major Application System Security Plan, which includes an ADBMS System Security Plan, on November 15, 2000. The plans were submitted to the Office of the Chief Information Officer. These plans are in compliance with the CIO's Computer Security Handbook All major application and the GSS SSPs are currently being modified to comply with the OCIO SSP reviews and are scheduled to be completed by November 15, 2001. Once these updates are completed for the Legacy systems that are being replaced by the MSIS, there will be no significant changes to these systems. Although the MSIS is scheduled for completion by the end of 2002, a delay in that date will certainly not be more than the three year update requirement.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.4)
Authorize Processing – Certification and Accreditation

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.5)
System Security Plan

MSHA Response:

The DOL CSH states that "The SSP should be updated on the basis of the subsequent mitigation activity or plan, after a significant system configuration change or every three years."

MSHA completed a General Support System Security Plan and a Major Application System Security Plan, which includes an ADBMS System Security Plan, on November 15, 2000. The plans were submitted to the Office of the Chief Information Officer. These plans are in compliance with the CIO's Computer Security Handbook All major application and the GSS SSPs are currently being modified to comply with the OCIO SSP reviews and are scheduled to be completed by November 15, 2001. Once these updates are completed for the Legacy systems that are being replaced by the MSIS, there will be no significant changes to these systems. Although the MSIS is scheduled for completion by the end of 2002, a delay in that date will certainly not be more than the three year update requirement.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.1)
Personnel Security

MSHA Response:

MSHA cannot mandate vacations for Federal employees. As an alternative, "job shift rotations" may be effective in very large organizations with significant depth in each position. MSHA's LAN staff is fairly small, so most staff are already replacing others when they are out. This is impractical to implement.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.2)
Physical and Environmental Protection

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.3)
Production, Input/Output Controls

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.4)
Contingency Planning

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.5)
Hardware and System Software Maintenance

MSHA Response:

MSHA's actions and plans meet this requirement, no response necessary.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.6)
Data Integrity

MSHA Response:

MSHA's actions and plans meet this requirement, no response necessary.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.7)
Documentation

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.8)
Security Awareness, Training and Education

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.9)
Incident Response Capability

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.3.1)
Identification and Authentication

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.3.2
Logical Access Controls

MSHA Response:

MSHA agrees with the OIG conclusion.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.3.3)
Audit Trails

MSHA Response:

MSHA agrees with the OIG conclusion.